STATE of ARIZONA

Arizona **D**epartment **O**f **A**dministration	**Agency** **STANDARD** **A800-O2-S04** **Rev 3**	**TITLE: ADOA Data Center Physical Protection – Physical Access Control** **Effective: September 3, 2010**

1. AUTHORITY

1.1. The authority for this Standard is based on Arizona Revised Statute 41-703 and the ADOA Policy A800 – Information Security Policy.

2. PURPOSE

2.1. The purpose of this Standard is to establish the responsibilities and restrictions to be complied with by all users of ADOA Information Resources.

3. SCOPE

3.1. This Standard applies to all ADOA employees, contractors and other entities using ADOA Information Resources.

3.2. The ADOA Director, in conjunction with the ADOA Chief Information Officer (CIO) and the ADOA Information Security (AIS) Manager, is responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies and Standards.

4. DEFINITIONS AND ABBREVIATIONS

4.1. **ADOA –** Arizona Department of Administration

4.2. **AIS –** ADOA Information Security

4.3. **AIS Manager** – ADOA Information Security Manager

4.4. **Authorized Personnel –** all individuals approved by AIS to access the ADOA Data Center facilities. These include full/part-time ADOA/State employees, temporary employees, contract employees and non-employees providing or receiving services or products to or from ADOA.

4.5. **Information Resource** - any computing device, peripheral (e.g., printers, scanners, USB flash drives), software, local and wide area networks(LAN and WAN), communications equipment (including Fax machines and telephones), communications software (including Internet, Intranet, and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities and data distribution, electronic data or related consumable (e.g. paper, disk space, central processor time, network bandwidth), information and data owned or controlled by the ADOA.

4.6. **Reception Area** – Lobby area at the south entrance of the ADOA Data Center where the initial contact between the public and department occurs, information exchanged, and visitor badge services are provided.

4.7. **Visitor –** Personnel requiring access into the ADOA Data Center and not carrying a badge issued to them that grants access into the secured locations within the ADOA Data Center

5. STANDARD

5.1. ADOA Information Resources, including critical information systems such as mainframes and servers, media storage areas, and communication wiring and network devices within the ADOA Data Center, will be situated in secure areas that are locked and restricted to badge access by authorized personnel only.

5.2. Badge access to secured areas will be granted by AIS.

5.3. Visitors requiring access to ADOA Data Center beyond the reception area will be signed in and out by authorized personnel and must obtain a Visitor badge.

5.4. To obtain a Visitor badge, a visitor MUST submit a valid State issued ID to the Capitol Police personnel at the ADOA Data Center South entrance. The Capitol Police personnel will validate visitor identity and issue a Visitor badge. Capitol Police will retain the State issued ID until visitor returns the Visitor badge, prior to exiting the facility.

5.5. Authorized personnel must escort visitors at all times.

5.6. Non-authorized personnel requiring access to ADOA Data Center areas beyond the reception area for extended lengths of time can request a limited access badge (“Red Badge”). A Red badge allows access only to areas required to perform work, allows the wearer to escort co-workers with Visitor badges and expires upon completion of work.

5.7. To obtain a Red badge, a written request must be submitted to AIS and the *Protecting Electronic Information* and *UNAX* classes must be completed.

5.8. Capital police will retain the AIS issued Red badge until access is required. To obtain the badge upon entry, a State issued ID must be submitted and retained while the Red badge holder is in the facility. Upon exit, the Red badge must be returned and the State ID will be given back. When the work is completed, the badge will be disabled and retained by AIS.

5.9. All laptops entering or exiting the Data Center must be reported to the guard on duty, inspected, and logged for identification purposes. All other electronic data storage devices may be inspected, and logged for identification purposes by the guard on duty.

5.10. All personnel will be subject to access monitoring that establishes the identity of the persons entering/exiting, as well as the date and time of the access (e.g., recording badge information, videotaping).

5.11. Where locking mechanisms with keypads are used to access secure areas, entry codes will be changed periodically, according to a schedule defined by the AIS.

5.12. Authorized personnel must individually register entry into areas by touching ID badge to the badge reader. “Tailgating” or “Piggy-backing is prohibited.

5.13. Unused keys and/or entry devices will be secured and usage tracked.

5.14. Physical access to critical IT hardware, wiring and network devices will be in accordance with ADOA Standard A800-O1-S01, Personnel Security, and controlled by rules of least privilege necessary for the authorized employee or contractor to complete assigned tasks. Logical access to critical IT hardware and network devices will be in accordance with ADOA Standard A800-T2-S01, Access Control.

5.15. All work areas and walkways must be kept clean and free of debris. Upon completion of any work in the room, personnel performing the work should ensure they have left the area as clean as it was before their work began.

5.16. Areas outside of rack enclosures shall be kept neat and free of manuals, diskettes, unused cables, spare equipment, and empty boxes. Doors on all racks should remain closed at all times except during performed work.

5.17. Cables should never be strung outside of rack enclosures or cable trays. Cabling between rack enclosures of adjacent racks is accepted provided sufficient pass-through chassis are in place.

5.18. All food and beverages are banned within the ADOA Data Center computer rooms. Under no circumstances should food or beverage of any kind be brought into the computer rooms.

5.19. Under no circumstances should anyone, without prior knowledge, consent, and oversight of the ADOA Data Center Operations staff:

a. Lift computer room floor tiles

b. Handle a Power Distribution Unit (PDU)

c. Handle a Computer Room Air Conditioning Unit (CRAC)

d. Open a communications cabinet or telecom closet door

e. Plug any device into another cabinet’s power supply

5.20. Signage throughout the data center shall adhere to the following color-coding standards:

- Red = restricted area or safety issue (i.e. authorized personnel only)
- Yellow = electrical (i.e. do not store items in front of electrical panel)

- Blue = notification (i.e. all personnel must show identification)

6. STANDARD NON-COMPLIANCE

6.1. All authorized users of ADOA Information Resources are responsible for understanding and adhering to this standard.

6.2. For non-compliance with this standard, all ADOA employees shall be subject to Human Resource progressive discipline, with the understood exception, that management may choose to take appropriate action commensurate with the seriousness of the offense.

6.3. Contractors and other authorized users will be held to contractual agreements.

7. REFERENCES

7.1. Statewide Policy – P800, IT Security

7.2. ADOA Policy – A800, Information Security

7.3. ADOA Standard – A800-O1-S01, Personnel Security

7.4. ADOA Standard – A800-T2-S01, Access Control

8. ATTACHMENTS

8.1. None